Published: Feb. 22, 2016, *Kokomo Tribune* [Page: A3]

http://www.kokomotribune.com/news/question-time-apple-vs-fbi-in-phone-fight/article_0a504928-d8f1-11e5-8725-fffcf8249be8.html

Question Time: Apple vs. FBI in phone fight

Should company comply with court order?

By Rob Burgess
Tribune night editor

[**Editor's note**: To participate in future queries, keep an eye on our Twitter and Facebook accounts.]

On Dec. 2, 2015, husband and wife, Syed Rizwan Farook and Tashfeen Malik, perpetrated a mass shooting at a San Bernardino County Department of Public Health holiday party in the Inland Regional Center in San Bernadino, California. Though not directed by the Islamic State, the couple's terrorist attack was inspired by their ideology. The massacre left 14 dead and 22 injured before Farook and Malik were killed hours later in a shootout with police.

A pair of destroyed personal cellphones were found discarded near the couple's home. However, an Apple iPhone 5C issued by the county to Farook was successfully recovered. Earlier this month, Federal Bureau of Investigations Director James Comey announced they were unsuccessful in unlocking the phone, which has a passcode. On Feb. 16, the FBI

successfully filed a motion in the United States District Court for the Central District of California under the All Writs Act of 1789. The motion asked Apple to provide “reasonable technical assistance” to create a new version of its iOS software which could be used by the government to bypass the phone’s security without wiping the data.

The same day, Apple CEO Tim Cook issued an open “Customer Letter” explaining their decision not to comply with the order.

"Some would argue that building a backdoor for just one iPhone is a simple, clean-cut solution,” he wrote. “But it ignores both the basics of digital security and the significance of what the government is demanding in this case. In today’s digital world, the ‘key’ to an encrypted system is a piece of information that unlocks the data, and it is only as secure as the protections around it. Once the information is known, or a way to bypass the code is revealed, the encryption can be defeated by anyone with that knowledge. The government suggests this tool could only be used once, on one phone. But that’s simply not true. Once created, the technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks — from restaurants and banks to stores and homes. No reasonable person would find that acceptable."

On Friday, the Department of Justice filed a new motion asking the court to force Apple to comply with the previous order, calling Apple’s stance a

“marketing ploy.” Apple responded by saying other options of accessing the phone’s data had been ignored or rendered obsolete.

“Apple said that in early January it provided four alternatives to access data from the iPhone besides the controversial method the FBI is now proposing,” reported The Los Angeles Times’ Paresh Dave on Friday. “But one of the most encouraging options was ruled out because within 24 hours of the shooting rampage, the phone’s owner — possibly Farook’s employer, the San Bernardino County public health department — reset the password to Farook’s iCloud account to access data from the backup, according to Apple and federal officials. That means the iCloud password on the iPhone itself is now wrong, and it won’t back up unless someone can get past the phone’s passcode and change it. The issue was discovered after Apple engineers sent to Southern California to work with the FBI struggled to trigger an automatic backup, Apple said. When iCloud is enabled, iPhones automatically sync with the cloud if they are charging and are connected to a familiar Wi-Fi network.”

So, we wanted to know: “Do you think Apple should comply? Why or why not?”

YES

“When did the terrorist have more rights in our country then we do? They can bomb us, kill lots of people and, hey, it's OK evidently. Wow. This sure

isn't the America I grew up in. One day we won't be here at all.” — **Georgiana M. Lamb**

“Yes, they should comply. How would this create a breach if only given for Apples, use on one iPhone?” — **Dianne Snow Huffer**

“They do not deserve any rights. Apple executives: Jail them, ‘til they do it!” — **Connie White**

“The provisions of the Fourth Amendment have been fully met. The Constitution doesn't protect dead people, anyway. … The request is for a method to bypass the provision (possibly built in to the A7 chip that runs the phone) that erases it after [10] unsuccessful PIN attempts. This requires the physical phone (so no over-the-air threat) and a physical connection to a computer running the requested software. Apple can manage the computer and the software any way they want — all they have to do is provide the PIN to the FBI. … Tim [Cook claims] that the government is asking them to build in a back door. There is no Constitutional issue here — the government has always had the right to ‘invade’ peoples' privacy under special circumstances. And there are no absolute rights guaranteed in the Constitution. Given the government's disinterest in preventing jihad in this country, I think the FBI and the judge who issued the order are to be commended for wanting to learn what they can from a dead terrorist — who, by the way, has no rights of any kind, including a right to privacy. … I

don't see how Apple can continue to stonewall. Time for contempt proceedings and jail time.” — **Steve Jones**

“Apple has been asked to provide particular info on this one county government phone which was used by a terrorist. I bet the Apple records for getting into the phone help with getting out of the phone. All Apple has been instructed to do is to release the info on the phone — no computer programs, etc. The application for this warrant is no different than the government seeking a search warrant for a private home. Apple is using this incident as good advertising for its phone. I bet criminals, terrorists, liars such as marital cheaters are pleased as punch with Apple's response to this. … Let them hack their own ultra-secure product and give the FBI the data of a dead man. Again, this is about publicity and profit for Apple. It has nothing to do with security for the common man.” — **Debbie Jones**

“Apple has the right to seek appellate review of the court's order and has articulated a legitimate interest in maintaining the privacy of its clients and the security of its systems. The government likewise has an interest in seeking the data and it is proper that the issues are argued fully before an appellate court so the competing interests can be balanced by a fully informed tribunal. Nobody commenting here has access to all the facts that the court will have. We should all be happy that these matters are decided in court and not by polls or on Facebook.” — **Dan Egbers**

NO

“No. It gives the government too much power and creates a way for others to hack into any iPhone.” — **Juanito Enrique**

“This is not about the rights of terrorists. This is about creating a program that could be used on any phone. If they crack one, it can be applied to any other phone using the same operating system. Once this program is created, then who owns it? The government? Apple? They could hack into any iOS phone with ease once this is created. This is not about protecting the rights of terrorist groups. This is about protecting the rights and expectation of privacy of the average American. Plus, the judge's orders only required that they ‘reasonably’ assist the FBI. Damaging their own security they've built for all their users is not reasonable. … The phone is encrypted. Call history, texts, etc. get encrypted when they're put on the server. Without the password, the only way to get the information off the phone is to hack it. The way you hack it is to create a back door into the iOS program (which could be applied to any phone running said iOS program, and in the wrong hands very dangerous). They do this so it's a lot more difficult for people (perhaps even terrorists) to hack your phone and get your bank password or any other sensitive information people keep on their phones these days. I hate Apple. I own zero Apple products and probably never will. They are right to refuse.” — **Gwen Indrutz**

“Everyone is up in arms about the Second Amendment and guns. Can we get as upset about the Fourth, please?” — **Kat Miller**

“Can only guess, but guessing anyway that a chain of custody is involved. In other words, the government wants the tool, and does not want Apple to do the unlocking as this might introduce data to the phone not originally on it. But, that tool could be used on other phones without Apple's knowledge.” — **Ernie Stamper**

“I understand why we/the government wants this info. My concern is where it will stop. Will it be used against you or someone in your family? Probably not. I personally don't want to take this chance.” — **Jim Tresenriter**

“I have to think that Tim Cook is better aware of the implications of the technology required to access the information on the iPhone than we are. It is Mr. Cook's world.” — **Gordon Slone**

OUR ANSWERS

“When it comes to national security I feel there should be exceptions. If one of my family members (or our president) was murdered by someone that these criminals had communication with and could be found on their phone I would be crazy mad! After all … if you’re not communicating with terrorists — dealing drugs, etc. — why worry about what’s to hide?” — **Sue Erny**

“I will quote the Fourth Amendment to the U.S. Constitution: People shall be ‘secure in their persons, houses, papers, and effects, against unreasonable searches and seizures...’ Handing the government what

amounts to a skeleton key able to unlock anyone's cellphone seems to go against the spirit of this amendment, so no, I don't think Apple should provide such a backdoor security breach.” — **Sarah Einselen**

“This is a fascinating case with implications far beyond this one particular event. It’s a tough one because you’ve basically got two authoritarian regimes fighting for control. On the one hand, you have the government, who would like nothing more than to have the ability to bypass Apple’s encryption on not just this device, but any locked iPhone. On the other hand you have Apple, which, in this instance, has everything to gain reputation-wise by acting as a bulwark between the trading of privacy for security. As the terrorists went to great lengths to destroy their personal devices, but left this work phone untouched, it says to me that there’s probably nothing of interest on this phone. And, as I’ve seen digital security expert Jonathan Zdziarski point out, the government didn’t exactly do everything they could to access this information without resorting to the current state of affairs. ‘FBI turning iPhone off: 1. Disabled Siri. 2. Locked most of the crypto. 3. Eliminated network capture option. 4. Eliminated runtime exploitation,’ he wrote on Twitter on Saturday. The real question is: Should private companies and citizens be able to produce un-pickable locks? As someone who has had his identity stolen before, I’d tend to say yes. But, what about cases like this one where the lock isn’t able to be picked because no one has yet made a key? I think Apple is completely justified in denying this order as the modified iOS would be out of their hands once they comply. The chain of

custody would be broken, but the only way I see them being able to 'reasonably assist' the government would be for Apple to have complete control of the phone while the data is being extracted and then be able to destroy the device and new iOS after. That would never happen, so I guess my answer would have to be no." — **Rob Burgess**

Rob Burgess, Tribune night editor, may be reached by calling 765-454-8577, via email at rob.burgess@kokomotribune.com or on Twitter at twitter.com/robaburg.